THE CYBERSECURITY WORKFORCE PLANNING DIAGNOSTIC

Interactive diagnostic tool:
Building on foundational workforce planning guidance

Homeland Security

Next

Cybersecurity Workforce Planning

Workforce planning is a key process for filling the gaps in an organization's cybersecurity workforce.

The need for cybersecurity specialists is growing exponentially due to increasing criminal, state-sponsored, and terrorist threats. Currently, there are not enough cybersecurity professionals to meet the volume and ever-changing nature of cybersecurity work. Compounding the gap between need and available workforce is the length of time cybersecurity specialists need to adequately develop the necessary skills. The cybersecurity field necessitates that its practitioners grow, evolve, and maintain highly-technical skills that take a significant amount of time to mature. Therefore, it is imperative that organizations practice effective *workforce planning* in cybersecurity.

Effective workforce planning enables organizations to build processes that not only identify where major cybersecurity gaps reside, but also pinpoint where an organization should proactively grow and shape its cybersecurity workforce to achieve mission priorities.

The purpose of this tool is to introduce a qualitative management aid to help organizations identify the data they need to gather to execute effective cybersecurity workforce planning. By considering implications of specific organizational characteristics around two factors– risk exposure (as a function of mission cyber security dependence aligned to compliance standards) and risk tolerance– organizations will gain insight into what types of data they need to better plan for and manage their **cybersecurity workforce.**

This tool will enable organizations to make data-driven decisions in regard to resource allocation and human capital infrastructure investments to support an organization's overall ability to meet its mission responsibilities.

Next

Before You Begin

This is an interactive tool to determine the data needed to support effective workforce planning for your organization.

Instructions:

Computer settings: You do **NOT** need to have Java enabled to use this tool.

Use the next arrow button on the bottom of each page to navigate though the tool. Next

The following table of contents also serves a home page allowing you to navigate to specific sections.

To return to the table of contents, click the home button.

If you save this document to your hard drive, you will have to clear your data (i.e., uncheck the Yes/No boxes) each time you use the diagnostic tool.

Throughout the tool, there are additional links that provide helpful information.

Next

The Cybersecurity Workforce Planning Diagnostic

Next

Evaluating Cybersecurity Workforce Planning Data Needs

Cybersecurity experts agree that the main consideration in planning for future cybersecurity personnel and infrastructure need is an organization's cybersecurity risk equation.

Evaluating workforce planning data needs: Risk has many dimensions. For the purpose of this tool, cybersecurity and workforce experts define the concept of risk through two elements:

1. ***Risk Exposure: the likelihood that a threat will occur (Threat), and***
2. ***Risk Tolerance: the likelihood that the threat will succeed (Impact).***

The resulting analysis of threat versus impact allows an organization to determine: 1) whether they can accept potential cybersecurity outcomes, or 2) if they must take action to mitigate those outcomes. When examined together, these two factors – *risk exposure* and *risk tolerance* – create a baseline organizations can use to evaluate cybersecurity workforce planning data needs.

Next

A Qualitative Management Tool

This qualitative management tool is intended to supplement and build upon previous national workforce planning efforts (focusing on talent management).

Using the concepts of risk exposure and risk tolerance will help organizations determine the types of organizational data necessary to execute their cybersecurity workforce planning process.

The **Cybersecurity Workforce Planning Diagnostic Tool** provides organizations with:

1. A *qualitative tool* to identify their cybersecurity risk exposure and their willingness to take on greater cybersecurity risk (risk tolerance) due to the nature of their organization and the types of activities in which they engage.
2. Placement within a quadrant aligning to one of four potential risk exposure/risk tolerance types: *low risk/low tolerance; high risk/high tolerance; high risk/low tolerance; and low risk/high tolerance. (*After completing the diagnostic, organizations can tally their combined risk exposure and risk tolerance score, and subsequently place themselves into a risk exposure/risk tolerance quadrant).
3. *Specific guidelines on the type of data an organization needs to collect* to perform effective cybersecurity workforce planning processes (e.g., analyze gaps and identify future workforce needs) based on the risk exposure/risk tolerance type.

To get the most use out of the Diagnostic tool, it is recommended that users review foundational resources on cybersecurity workforce planning:

1. *Best Practices for Planning your Cybersecurity Workforce* white paper
2. *Cybersecurity Capability Maturity Model* white paper located on the National Initiative for Cybersecurity and Career Studies (NICCS) portal.

Next

What is Risk Exposure?

Risk exposure *measures the level of cybersecurity risk an organization incurs based on its mission operations, support infrastructure, security architecture (i.e., people, policy, process and technology), partnering relationships, type of work or service performed by employees, and its relative business imperatives (i.e., the major goal and/or purpose of the business).*

This risk may be inevitable given an organization's business mission (i.e., banks must conduct business over the internet) or it may be an acceptable choice based on level of risk tolerance.

Risk exposure:

1. Qualifies the potential likelihood of a cybersecurity event for an organization based on certain factors (including mission, type of workforce, work performed);
2. Drives the type and amount of work an organization will need to accomplish to properly safeguard itself from possible attacks and intrusions (based on the criticality of the cyber environment to business/mission success);
3. Influences the type and number of cybersecurity professionals an organization needs.

To better understand your organization's risk exposure, go to the risk exposure questionnaire or click the "Next" arrow to earn about **risk tolerance** and how it relates to risk exposure.

Next

What is Risk Tolerance?

Risk tolerance *measures an organization's attitude towards risk, or its ability to absorb and/or accept risk based on the operational impact of an event on business/mission operations.*

This risk varies given an organization's willingness to accept threat exposure based on business decisions for acceptable risk levels, risk impacts, and required resource impacts in preparing to handle possible enterprise attacks. These factors translate to specific types and numbers of personnel, and skills and training for cybersecurity professionals needed to protect organizational cyber environments.

Risk tolerance:

1. Drives the threat-mitigating solutions, and related work, an organization develops to respond to exposure risks;
2. Influences the number and mix of cybersecurity staff an organization employs;
3. Allows organizations to perform meaningful workforce analysis for its cybersecurity workforce.

To better understand your organization's risk tolerance, go to the risk tolerance questionnaire or click the "Next" arrow to learn about workforce planning.

Next

Workforce Planning – Overview

Workforce planning *is a systematic way for organizations to identify current human capital capabilities (supply), determine future human capital requirements (demand), and design and implement strategies to transition the current workforce to the desired future workforce. Effective workforce planning is designed to be repeatable and reliable, highlighting risks and forecasting needs over time.*

Effective workforce planning highlights potential risk areas associated with aligning workforce to work. Applied correctly, workforce planning allows organizations to adjust resources to meet future workloads, patterns of work, and fundamental changes in how work is accomplished. A workforce planning approach must fit the needs of a specific organization and account for unique characteristics of the cybersecurity profession.

Best practice workforce planning consists of three components:

1. **Process:** Establishing an integrated and consistent means of diagnosing workforce needs and risks. This includes a defined model, data and analytics.
2. **Strategy:** Providing a direct line of sight between business and workforce requirements. This includes a shared vision, governance, and continuous monitoring or performance.
3. **Infrastructure:** Supporting execution of an effective and repeatable workforce planning process. This includes a strong workforce and collaboration across technology.

A **workforce planning process,** as described on the following page, identifies and quantifies the workload and workforce requirements unique to an organization; and analyzes the skills needed to fill the gap in the workforce.

Next

Workforce Planning – Overview

As the demands of global business, computing, and society revolve around information technology, the cybersecurity workload is increasing faster than cybersecurity professionals can meet the demand. As such, an emerging priority in cybersecurity is how organizations can attract, assess, and develop this specialized workforce.

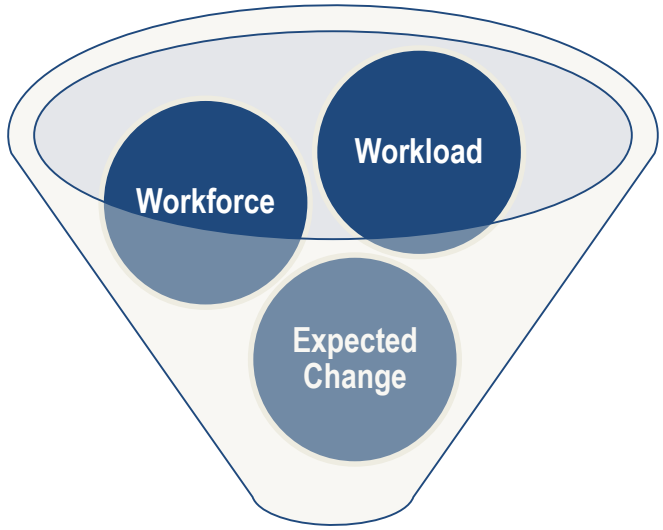
Workforce planning is the process organizations can use to address these concerns. Workforce planning analyzes demand issues and helps organizations close the workforce gap in a systematic way.

Workforce planning helps answer:

- ✓ What does our current workforce look like?
- ✓ How many cybersecurity workers do we have?
- ✓ What positions do these individuals hold?
- ✓ What is their current workload?

Workforce planning informs decisions organizations make to correctly plan for the future:

- ✓ Do we anticipate changes in workload?
- ✓ Are our workers correctly aligned to the work?
- ✓ Is additional training needed if the work is changing? Are new positions needed?
- ✓ Do we have the budget to fund the positions needed to meet our goals and objectives?

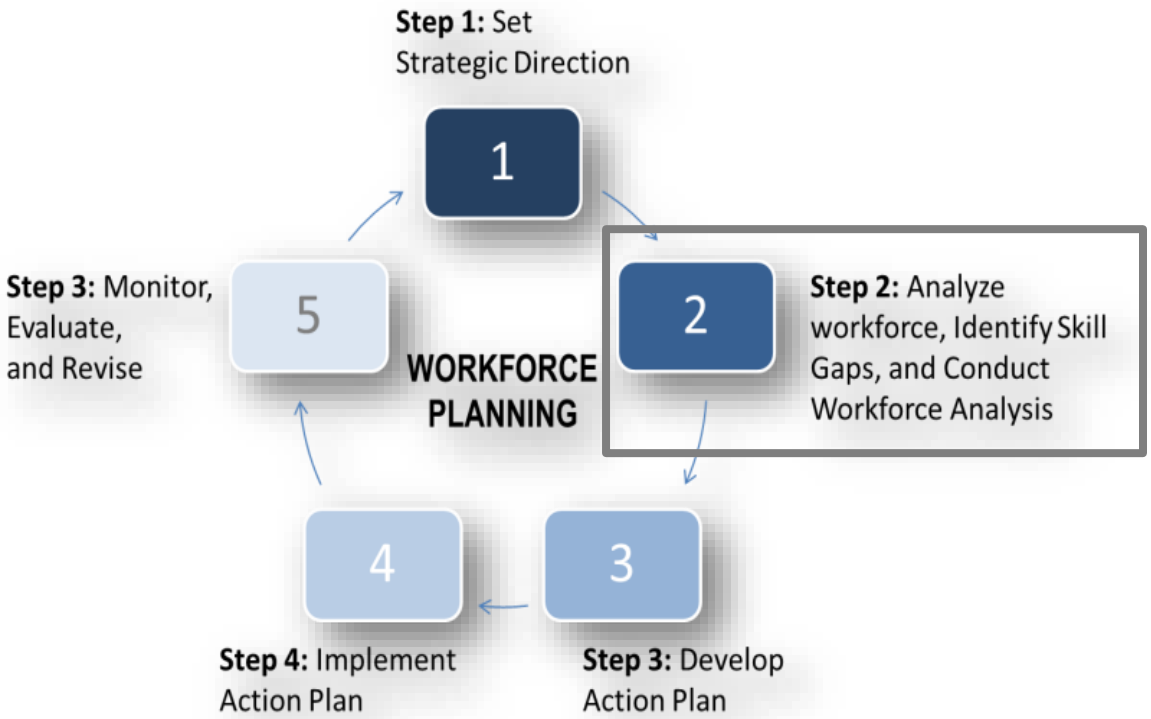


Workforce Planning and Analysis

Next

Workforce Planning – Using the Diagnostic Tool

Workforce Planning Process



This diagnostic tool focuses on analyzing cybersecurity supply and demand data as it relates to risk factors (see **Step 2** of the workforce planning process graphic).

Additional details on workforce planning best practices, capability maturity, and other process components can be found in the workforce planning section of the NICCS portal.

Next

Introduction to the Cybersecurity Workforce Planning Diagnostic

The Cybersecurity Workforce Planning Diagnostic characterizes organizations by their ***responses to risk exposure and risk tolerance questions*** to help identify an organization's practices towards risk from internal exposure (e.g., poor cybersecurity monitoring and controls reporting), external exposure (e.g., threat actor cyber intrusions) and the amount of risk an organization is willing to accept.

By identifying current organizational cybersecurity risk exposure and cybersecurity risk tolerance behaviors, an organization can isolate the type of data it must collect to determine its future cybersecurity work (demand) and related necessary workforce (supply).

IMPORTANT NOTES:

- ✓ The Diagnostic will help organizations identify general cybersecurity risk exposure and risk tolerance. It is not a substitute for in-depth, organization-specific risk assessment and analysis– questions listed within the diagnostic are representative.
- ✓ There are several other factors not utilized in the Diagnostic (e.g., technological infrastructure, mission imperatives, and changing external platforms) that will impact an organization's ability to effectively meet its cybersecurity needs.
- ✓ Organizations can use Diagnostic questions to a create foundational knowledge about their cybersecurity workforce risk. Organizations can use this knowledge to create more questions based on their technical and specific mission imperatives, and organizational structures.
- ✓ Organizations should keep in mind that it will take the collaborative work of leadership, human capital experts, and cybersecurity managers and operators to accurately use the Diagnostic tool.

Next

Risk Exposure Questions

Regardless of the size of an entity, the amount of risk exposure an organization faces can influence the amount, type, and specific cybersecurity skills it needs to adequately protect itself and operate in cyberspace.

Organizational compliance is critical in safeguarding infrastructure, but compliance alone does not necessarily safeguard against all security breaches or cyber intrusions. Therefore, to identify cybersecurity professionals needed beyond its compliance baseline, organizations must consider additional factors of **risk exposure** – such as attack surface.

RISK EXPOSURE EXAMPLE:

An organization that conducts business with a foreign entity may expose itself to more risk in by compromising its intellectual capital compare to an organization that does not work with foreign entities. In conducting these business transactions it will likely answer yes to more risk exposure questions, and also tolerate a possible cybersecurity intrusion (i.e. tolerate more risk) because the benefits of doing business outweigh the negatives or impact of a cybersecurity incident. Thus, it will have a higher risk score.

The diagnostic risk exposure questions are divided into two sets. One set is for federal organizations and the other is for non-federal organizations:

Click one to continue

Federal risk exposure questions

Non-Federal risk exposure questions

Federal Risk Exposure Questions

Place an "X" in the box corresponding to each of your answers:

	Federal Risk Exposure	YES	NO
Federal Risk Exposure	1. Is your organization subject to standards, policies, or regulations dictated by external bodies or industry governance?		
	2. Is your organization subject to government-mandated cybersecurity policies and procedures?		
	3. Based on your organizational mission, is your organization permitted to operate outside government - related cybersecurity policies and procedures?		
	4. Based on organizational mission, is your organization permitted to operate outside industry-related policies and procedures?		
	5. Does your organization's business/mission require maintaining data that, if jeopardized, would impact privacy laws or policy guidelines?		
	6. Is your organization's mission related to national defense, law enforcement, or counterintelligence?		
	7. Is your organization's mission related to critical infrastructure?		
	8. Does your organization's mission directly support cybersecurity efforts?		
	9. Does your organization have a National cybersecurity role?		
	10. Can your organization account for all of its attack surfaces for the specific mission under consideration?		
	11. Does your organization have regular cybersecurity hygiene training for all its employees?		
	12. Does your organization protect access by granting graduated levels of IT clearances for employees?		
	13. Does your organization document and track successful and unsuccessful cybersecurity breaches?		
	14. Does your organization change its security posture once an attack/intrusion (regardless of success) occurs?		
	15. Is anyone on your leadership team part of U.S./external cybersecurity policy and protection discussions?		
	16. Does your organization engage in CNA (computer network attack) operations?		
	17. As a way to ensure integration and sharing of information pertaining to cybersecurity, does any part of your organization's workforce participate in job rotations or TDY (temporary duty)?		

Add up all the "NO" answers [ ]

The value in the red box is your **Risk Exposure score** to be used in mapping to the Risk Exposure / Risk Tolerance Matrix.

Next

Non-Federal Risk Exposure Questions

Place an "X" in the box corresponding to each of your answers:

	Non- Federal Risk Exposure	YES	NO
Non-Federal Risk Exposure	1. Can your organization account for all its attack surfaces?		
	2. Does your organization have regular cybersecurity hygiene training for all its employees?		
	3. Does your organization protect access by granting graduated levels of clearances for employees?		
	4. Does your organization document and track successful and unsuccessful cybersecurity breaches?		
	5. Does your organization change its security posture once an attack/intrusion (regardless of success) occurs?		
	6. Does your organization require employees to undergo background checks?		
	7. Does your organization employ foreign nationals?		
	8. Does your organization's mission require you to maintain sensitive data?		
	9. Does your organization have specialized operational cybersecurity workforce?		
	10. Does a part of your workforce possess unique cybersecurity skills, beyond those needed for cyber hygiene and information assurance, like malware analysis, digital forensics, reverse engineering, threat actor identification, or ethical hacking?		

Add up all the "NO" answers ☐

The value in the red box is your **Risk Tolerance score** to be used in mapping to the Risk Exposure / Risk Tolerance Matrix.

Next

Risk Tolerance Questions

An organization's **risk tolerance** influences the amount and type of cybersecurity skills an organization needs to adequately protect itself and operate in cyberspace

Organizations commonly use a measure of impact to determine the level of risk they are willing to tolerate. ***Impact*** refers to the level by which the organization is affected by a risk, and it is based on how greatly an organization's mission imperative, business proposition, or in some cases of federal agencies, national security, may be impaired/compromised.

Organizations routinely comply with existing security controls, but these mandates, laws, and policies are, at times, a minimum standard. Complying with these controls does not necessarily mean that organizations are fully protected or safeguarded from potential threats/attacks. Moreover, many organizations make calculated security decisions based on the cost of complying versus the cost of non-compliance.

Therefore, these organizations make a calculated tradeoff to accept more risk and have a high risk tolerance. For example, it may be more affordable to repair systems after an attack than harden the attack surfaces ahead of time. It is vital that organizations balance the need between baseline compliance and increased cybersecurity to minimize interruption to their respective business operations.

Click here to continue

Risk Tolerance questions

Risk Tolerance Questions

Place an "X" in the box corresponding to each of your answers:

	RISK TOLERANCE	YES	NO
Risk Tolerance	1. Has your organization identified specific threats/attacks that it can absorb (rather than address or mitigate) without damaging mission or business imperative?		
	2. Does your organization choose to plan for only some cybersecurity threats or risk?		
	3. Is there some data that your organization is willing to have breached as a cost to performing necessary business operations?		
	4. Does your organization make trade-offs (in allocation of resources to increase market share or profitability) rather than building more sophisticated cyber defenses?		
	5. Does your organization engage with external partners/entities (despite increased exposure to cyber-attacks or intrusions as a result of these dealings)?		
	6. Does your organization deliberately choose to be out of compliance with government/industry regulations because these regulations are more costly/inconvenient to follow than penalties for non-compliance?		
	7. Has your organization's cybersecurity infrastructure ,more or less, stayed the same for the last five years?		
	8. Has your organization's cybersecurity workforce (i.e., size and expertise level) more or less remained constant over the last five years?		
	9. Do you know what types of attacks present the greatest risk to your business / mission operations and success?		
	10. Is your cyber workforce prepared to "fight through" / address those attacks?		
	11. Does your workforce have the training to address those attacks?		
	12. Does your organization have a continuity of operations plan (COOP) plan for "fight through" / mission continuation, or under degraded conditions?		

Add up all the "YES" answers [ ]

The value in the red box is your **Risk Exposure score** to be used in mapping to the Risk Exposure / Risk Tolerance Matrix.

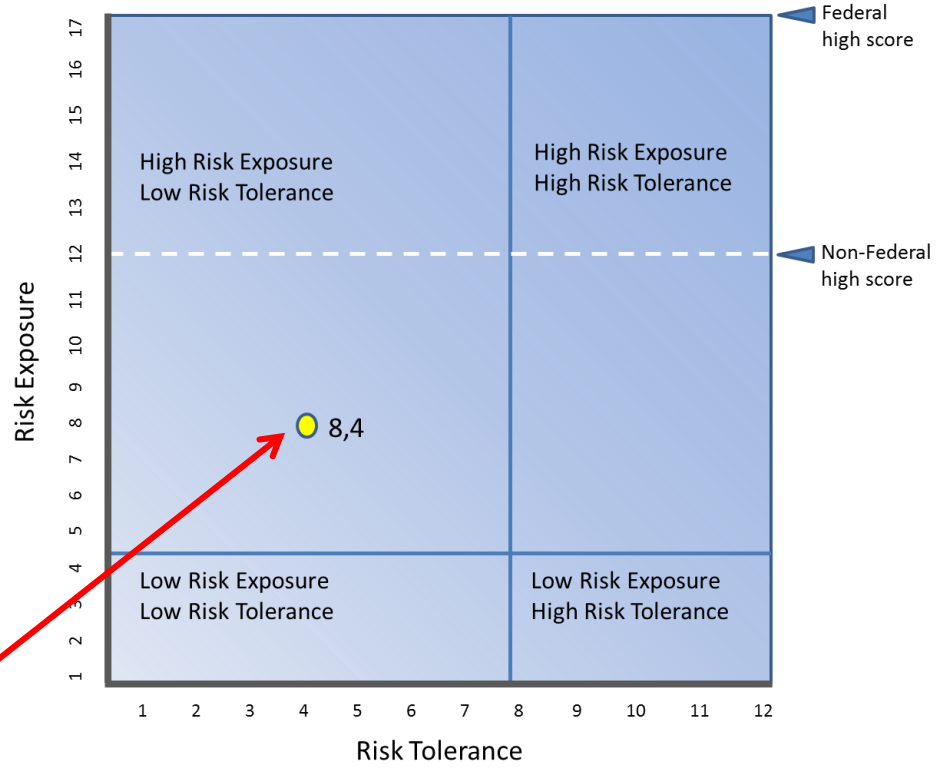
Next

Risk Exposure/ Risk Tolerance Diagnostic Matrix

To determine which quadrant you fall into, plot your organization's **risk exposure score on the vertical y-axis** and the **risk tolerance score on the horizontal x-axis**.

Based on responses to the diagnostic questions, your organization will fall into one of four risk exposure/risk tolerance quadrants:

1. Low Risk Exposure/Low Risk Tolerance
2. High Risk Exposure /High Risk Tolerance
3. High Risk Exposure /Low Risk Tolerance
4. Low Risk Exposure /High Risk Tolerance



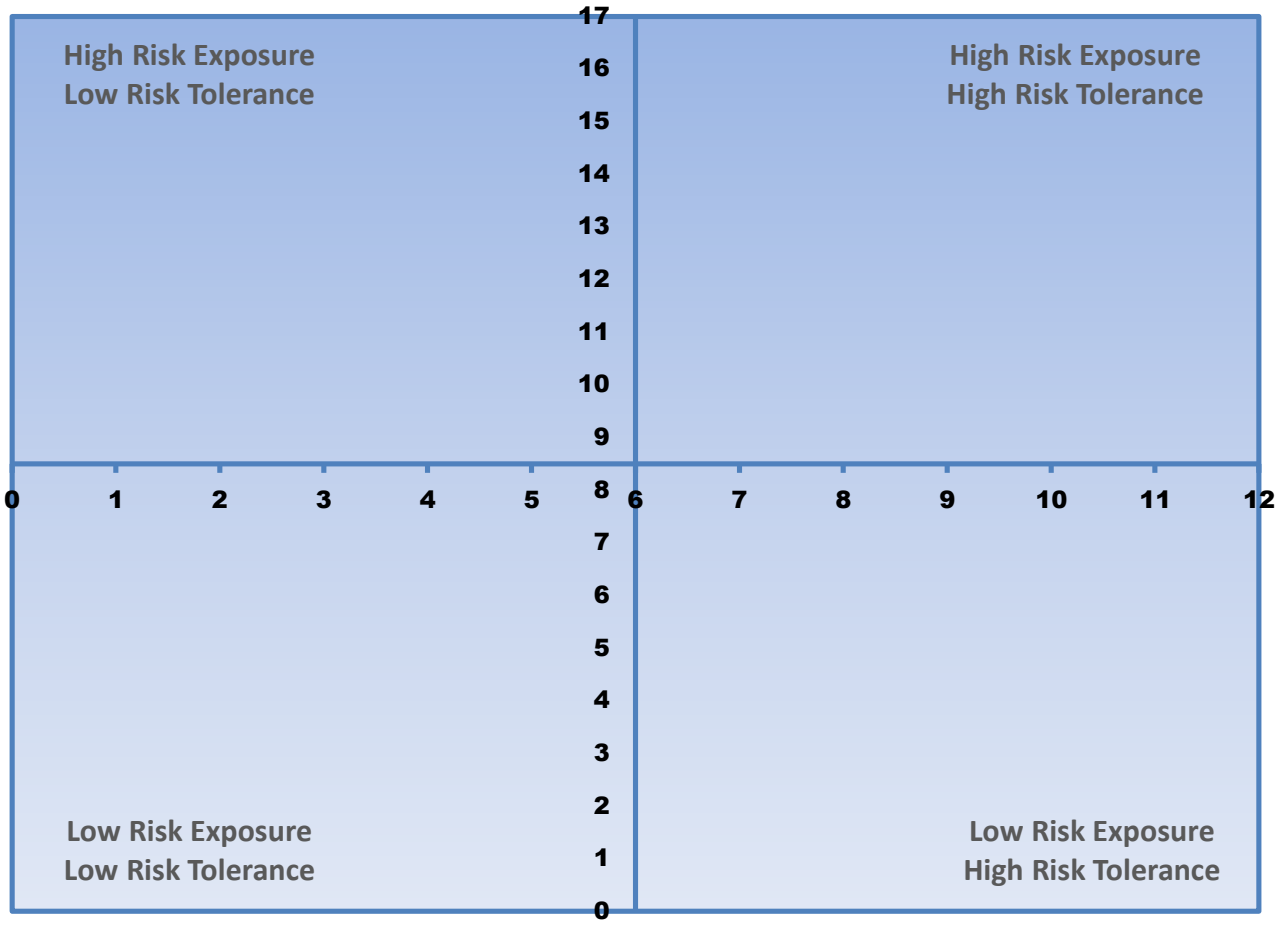
For example *to plot a risk exposure score of 8 and a risk tolerance score of 4, count up 8 from the bottom of the risk exposure numbers, then over 4 on the risk tolerance numbers to determine your position on the matrix.*

***Please click "Next" to plot your organization's risk exposure and risk tolerance score**

Next

Placement on the Diagnostic Matrix

To determine which quadrant you fall into, plot your organization's **risk exposure score on the vertical y-axis** and the **risk tolerance score on the horizontal x-axis**.



Next

Supply and Demand Data - Overview

Now that you know which quadrant your organization falls into on the matrix, the following information will help you understand the ***key considerations for establishing workforce planning practices***. These considerations include:

- ✓ ***data types (supply*)*** and,
- ✓ ***workload (demand)*** measurement methods.

The following sections provide guidance on how to conduct cybersecurity workforce planning. These sections are focused on supply data inputs and demand planning methods based on your organization's risk exposure/risk tolerance type.

**Federal government organizations can use the Information Technology Workforce Assessment for Cybersecurity (ITWAC) findings for some supply data. Non-Federal organizations can gather similar data from their own institutions to gain insight into their current cybersecurity supply.*

Next

Supply Data - Factors

As a reminder, the term *supply* refers to the individuals in the organization that fill cybersecurity positions, and their associated supply characteristics (e.g., retirement eligibility, occupational series, and grade/band/level).

Key notes when understanding an organization's supply data:

- ✓ Supply is not static - there is constant ebb and flow of employees into, across, and out of organizations.
- ✓ Workforce supply may change over time due to turnover, promotions, internal movement, funding, and federal/contractor mix. Understanding these trends, as well as how they might change based on various factors, is essential. These changes provide insight into how an organization will have to shape its workforce to meet future demand and identify workforce supply gaps.
- ✓ Organizations should also consider supply calculations to include attrition analysis, retirement rate based on historical data, modeling promotion and other internal movement patterns, or conducting scenario planning for changes in workforce mix to ascertain the potential cybersecurity workforce supply.

Below are some Supply Factor Examples:

Supply Characteristics		Supply Calculations
• Occupational Series • Grade/Rank/Band/Level • Education level • Certifications • Retirement Eligibility • Permanent/Temporary	• Spoken languages • Contractor/Federal Employee/Military • Specialized skills • Geographical location • Vacant positions • Tenure	• Attrition rate • Turnover • Time to hire • Separation rate • Average retirement age • Recruitment/Succession pipeline

Next

Supply Data

Depending on an organization's risk exposure and risk tolerance, certain supply factors will be more important than others. The following are considerations for supply data based on which of the four quadrants an organization falls into:

Low Risk Exposure/Low Risk Tolerance

An organization that falls into the *low risk exposure / low risk tolerance* quadrant is one that is exposed to the least cybersecurity threats, but is also unwilling to absorb cybersecurity threats and intrusions. This means that it is highly unlikely that a cyber-attack will occur, but if one does, the impact could be severe to internal business/agency operations. Therefore, this organization will ensure measures are in place to protect its data and intellectual capital. For example, this organization may be represented as a domestically-owned, single proprietorship performing professional services to agencies or other organizations. Its data is not a likely target to outside threats, yet if the data was compromised in some way the organization would experience negative repercussions of significant impact levels. Click here to learn about the workforce planning implications for this quadrant.

High Risk Exposure/Low Risk Tolerance

An organization that falls into the *high risk exposure / low risk tolerance* quadrant has the highest exposure, yet the least tolerance of risk. This organization is likely a target of cyber-attack from multiple actors – those that seek to penetrate the organization's networks to prove their ability, to those actors that wish to steal data and/or severely disrupt the organization's capability. Knowing the possibility of attack and the likely impact, this organization makes decisions and takes deliberate actions to address many of the threats it faces. For example, this organization may be represented by an intelligence agency or military organization that possesses highly sensitive and classified data that, if exposed, would pose a serious national security breach. Click here to learn about the workforce planning implications for this quadrant.

High risk exposure/High risk tolerance and Low risk exposure/High risk tolerance……

Next

Supply Data (cont'd)

Depending on an organization's risk exposure and risk tolerance, certain supply factors will be more important than others. The following are some considerations for supply data based on which of the four quadrants an organization falls into:

High Risk Exposure/High Risk Tolerance

An organization that falls in the *high risk exposure / high risk tolerance* quadrant has the highest exposure and the highest tolerance of risk. This organization is a likely target for cyber-attacks of all kinds – from stealing of inconsequential data to protecting classified information – and as a result, the organization has to prioritize and make decisions around resource allocation to address the most impactful threats. For example, this organization may be represented by a national law enforcement agency with international partnerships and that holds a national cybersecurity role. Click here to learn about the workforce planning implications for this quadrant.

Low Risk Exposure/High Risk Tolerance

An organization that falls within the *low risk exposure / high risk tolerance* quadrant is one that is exposed to the least amount of cybersecurity threat, and is willing to absorb cybersecurity threats and intrusions. This categorization means that it is highly unlikely that a cyber-attack will occur, and if one does, the impact is relatively insignificant to internal business/agency operations. This organization is less likely to invest in cyber related safeguarding activities, and in many cases views the return on investment of these activities as low – resulting in little action. For example, this organization could be represented as a domestically-owned, single proprietorship, manufacturing and selling its good on the same premises. Click here to learn about the workforce planning implications for this quadrant.

Next

Supply Data Characteristics All Quadrants

Below are some examples of supply data characteristics within each quadrant:

Quadrant	Sample Supply Consideration
Low Risk Exposure/Low Risk Tolerance	*Characteristics:* education level *Calculations:* separation rate, permanent/temporary, military/civilian/federal
High Risk Exposure/Low Risk Tolerance	*Characteristics:* specialized cybersecurity certifications (e.g., ethical hacking, programming), retirement eligibility *Calculations:* time to hire statistics, succession pipeline, attrition rate
High Risk Exposure/High Risk Tolerance	*Characteristics:* occupational series, education level *Calculations:* permanent/temporary, military/civilian/federal, ratio of contractors/employees
Low Risk Exposure/High Risk Tolerance	*Characteristics:* occupational series, grade/level distribution (including supervisor level), tenure *Calculations:* ratio of contractors/employees

Next

Demand Data - Overview

As a reminder, *demand* refers to the amount and types of work an organization performs, and an organization's *demand for workforce* refers to the number, skill set, and experience mix of workforce needed to accomplish work. Accurately determining an organization's demand requires consideration of the scope, complexity, volume, and duration of its work.

Key notes when understanding an organization's demand data:

- ✓ Demand is not a constant.
- ✓ Develop an understanding of the work an organization does (including scope, complexity, volume, and duration tied to a project or a sub-organization's function.) This is necessary in order to assess current, and predict future, demand.
- ✓ Each aspect of an organization's cybersecurity work may be influenced by environmental or infrastructure factors. These factors provide insight into how its work may change and how the organization may have to shape its workforce to meet future demand.
- ✓ Consider demand drivers when conducting a **demand data analysis** in any workforce planning process. *Demand drivers* are quantifiable and measurable factors that influence the work performed. Organizations can numerically count demand drivers, as they are tangible things that impact, or drive, work (both in volume and complexity); and, each driver has an associated driver value (i.e., an actual number), which determines current demand or a baseline.
- ✓ It is possible to forecast future demand by using demand driver values in combination with environmental data, historical data, and leadership determinations.

Next

Demand Data - Drivers

Organizations can perform demand data analysis through priority-based demand planning. ***Priority-based demand planning*** *(also referred to as* ***threat assessment demand planning****)* is used when an organization has more work than resources available to accomplish it. As a result, leaders within that organization will make decisions based on mission goals/imperatives and risk tradeoffs regarding resource allocation.

Below are examples of cybersecurity demand data points. Note: It is not an exhaustive list as there are other factors that organizations can consider in demand planning.

Demand Drivers	
• Number of hardware items to maintain	• Historical number of cyber intrusions/attack
• Number of cyber help desk incidents	• Number of attack surfaces
• Number of personal identity verification (PIV) or computer access cards (CAC) to issue	• Number of external partners
	• Number of networks to monitor
• Number and type of regulations with which to comply	• Number of individuals with administrator rights
	• Types of threat
• Number of user accounts	• Number of likely cyber-attack actors
• Historical number of potential threats	• Level of impact (likelihood x probability) of cyber intrusion/attack
• Likelihood of threat occurrence	
• Cost-mission resource risk analysis/trade	• Number of specific event types/kinds of attack
• Type of architecture(s) within the enterprise	• Criticality of systems to mission success

Next

Demand Data

Depending on an organization's risk exposure and risk tolerance, certain demand factors will be more important than others. The following are some considerations for demand data based on which of the four quadrants an organization falls into:

Low Risk Exposure/Low Risk Tolerance

Organizations that fall into this quadrant (e.g., domestically-owned, single proprietorship performing services for local community) should consider quantifiable data inputs or demand drivers because the nature of their work is practicable and countable, and not based on risks or prioritization. Click here to learn about the workforce planning implications for this quadrant.

High Risk Exposure/Low Risk Tolerance

An organization that falls into this quadrant (e.g., international, intelligence agency) has many exploitable weaknesses, and invests in resources to prevent those weaknesses from becoming vulnerabilities. Consequently, this organization should do demand planning, primarily based on threat prioritization, because cybersecurity work is unpredictable in volume and pattern. Click here to learn about the workforce planning implications for this quadrant.

High risk exposure/High risk tolerance and Low risk exposure/High risk tolerance……

Next

Demand Data (cont'd)

Depending on an organization's risk exposure and risk tolerance, certain demand factors will be more important than others. The following are some considerations for demand data based on which of the four quadrants an organization falls into:

High Risk Exposure/High Risk Tolerance

An organization that falls in this quadrant (e.g., national law enforcement agency with international partnerships and national cybersecurity role) has the most stringent compliance standards and highest exposure to risk. The type of demand planning organizations within this quadrant will do is based on threat prioritization and less quantifiable demand drivers. Because the work is less predictable and by nature, these organizations will always have more work than they have personnel. Click here to learn about the workforce planning implications for this quadrant.

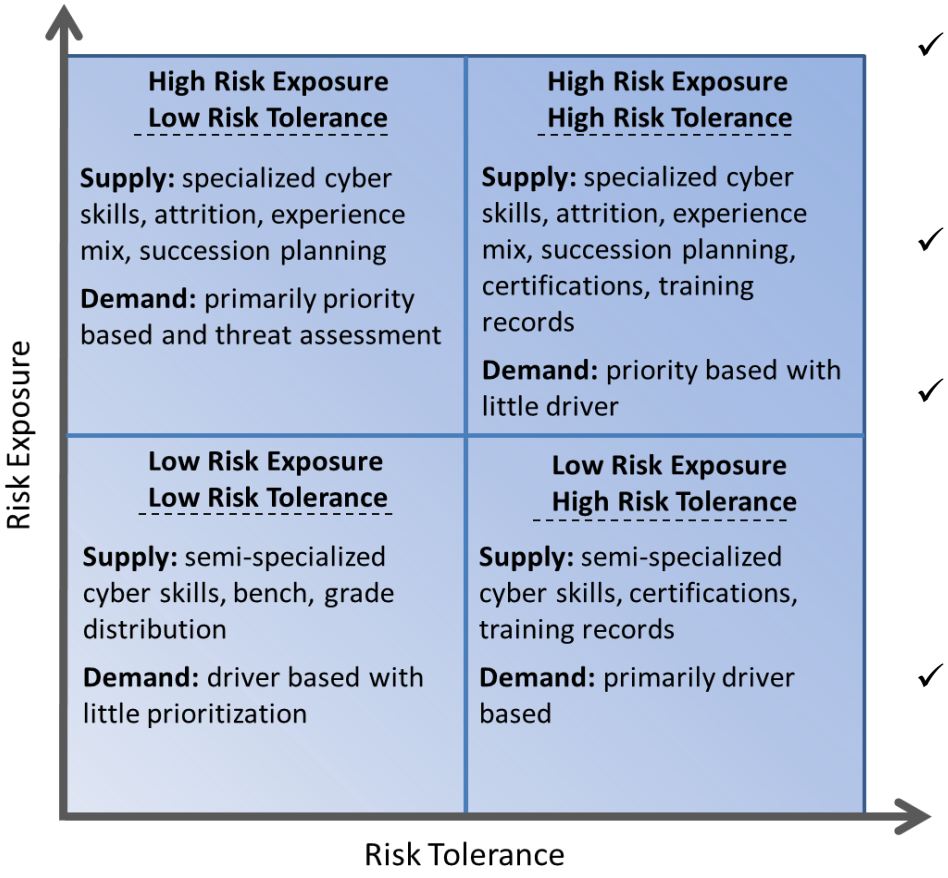
Low Risk Exposure/High Risk Tolerance

Organizations that fall into this quadrant (e.g., domestically-owned and operated mid-level organization, performing professional services with no need for supply chain) should also consider quantifiable data inputs or demand drivers. Similar to the low risk exposure, low risk tolerance organization, this organization's work is highly "countable" and the relationship between the volume of work and the amount of people performing it is a direct one (i.e., as the volume increases, the supply needed increases as well). However, this organization should consider additional demand data considerations due to its high tolerance designation, as it is more likely to absorb certain low impact cyber-attacks rather than invest to safeguard against them. Click here to learn about the workforce planning implications for this quadrant.

Next

Using Data to Support Decision Making

Understanding that organizations have finite resources restricting what data they can collect, the quadrants of the Cybersecurity Workforce Planning Diagnostic can help organizations better understand the types of data that will give them the greatest ROI.

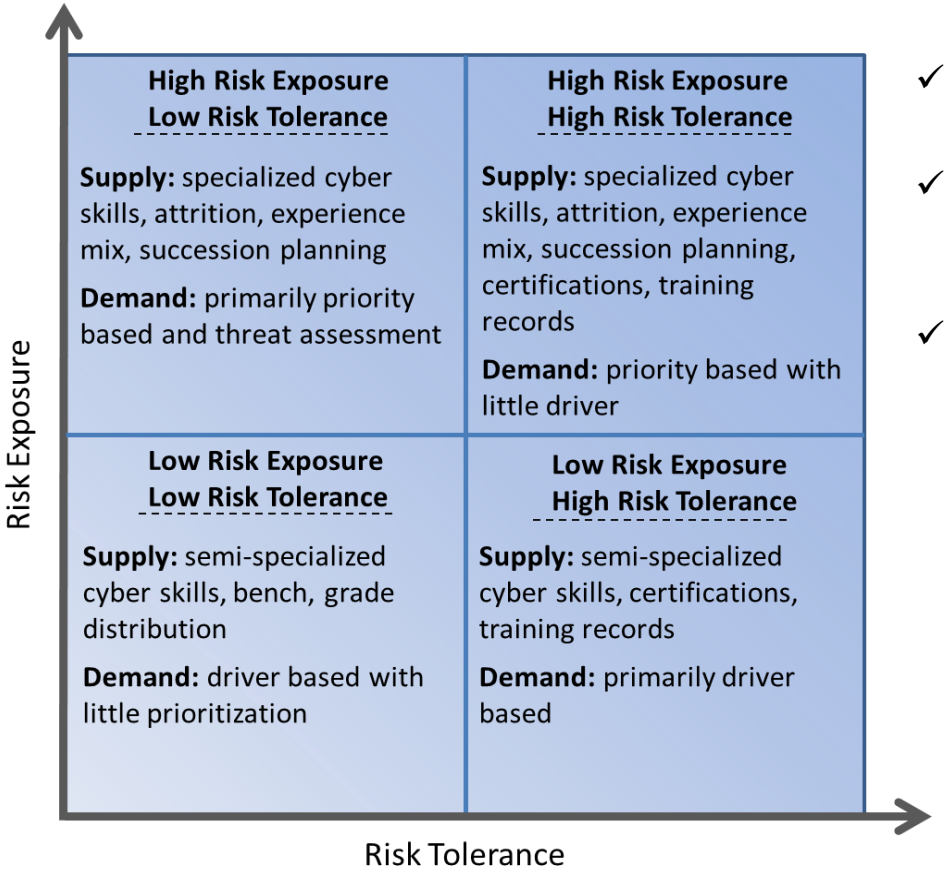


Supply and demand considerations by quadrant

- ✓ The quadrants provide a snapshot of the ideal considerations for organizations as it pertains to their cybersecurity workforce planning capability.
- ✓ They are aspirational suggestions on how organizations should perform supply and demand analysis.
- ✓ By taking these data considerations into account, organizations can tailor their approaches regarding workforce planning processes and mature their workforce planning capabilities in a more streamlined way.
- ✓ Through this increased understanding, organizations can make informed decisions around human capital investments and workforce planning strategy.

Next

Using Data to Support Decision Making (cont'd)



Supply and demand considerations by quadrant

- ✓ Workforce planning is only as good as the data that supports it.
- ✓ Understanding data needs also allows for consistent decision making and a decrease of redundant efforts.
- ✓ Finally, understanding data needs encourages integration across an organization and provides structure for a better understanding of what the entire organization – from headquarters to field offices – needs to stay safe and secure against attacks.

Next

Conclusion

By using the Diagnostic to benchmark organizational infrastructure along the lines of risk exposure and risk tolerance, organizations can more effectively evaluate their cybersecurity workforce supply and demand data needs. Organizations will have deeper insight into the workforce analytics that are needed to project future cybersecurity demand and complete a ***gap analysis between the current supply and future demand data***.

Although risk exposure/risk tolerance type will vary by organization size, scope, and cybersecurity complexity, the Diagnostic assists organizations by guiding them to key considerations in gathering supply and demand data based on their respective organizational profile. Business leaders, human capital practitioners, and other key cybersecurity personnel can use the outcomes of the Diagnostic as an initial assessment for organizational supply and demand factors, and better understand how those components interplay with the broader workforce planning strategy.

In conjunction with information provided in the ***Best Practices for Cybersecurity Workforce Planning White Paper***, and the ***Cybersecurity Capability Maturity Model (CMM) White Paper***, the Cybersecurity Workforce Planning Diagnostic tool provides organizations additional insights on compliance standards and risk exposure while building integrated workforce planning processes and data analytics.

Next

Information Technology Workforce Assessment for Cybersecurity (ITWAC)

The ITWAC is a workforce data collection tool to identify the composition and capabilities of the federal IT workforce executing cybersecurity responsibilities.

- ✓ The assessment was administered to federal departments and agencies to better understand the makeup of the cybersecurity workforce, baseline the national federal skill-set, and highlight the current proficiencies among the federal workforce.
- ✓ It provides workforce data that can support strategic human capital activities in cybersecurity training, workforce planning, and professional development. Departments and agencies can use their data to support these targeted activities related to building cybersecurity workforce capabilities.

The ITWAC Report (released March 2013) provides insight on:

- ✓ Occupational series, pay grades, years of experience, and many other cybersecurity workforce demographics;
- ✓ Certifications and education attained by the workforce;
- ✓ Current and optimal proficiency levels, and;
- ✓ Based upon current role, time spent in the 31 Specialty Areas of the National Cybersecurity Workforce Framework.

Using the Diagnostic, organizations can determine additional types of workforce and/or workload data they need to consider. With these data points, federal departments and agencies can better understand their current workforce, and shrink the gap between anticipated workload and to their needed future workforce.

Back to Supply Data

Supply Considerations - Low Risk Exposure/Low Risk Tolerance

Leaders within the ***Low Risk Exposure/Low Risk Tolerance*** organization can consider the following workforce implications:

- ✓ Cybersecurity activities are not central to the accomplishment of its mission, but rather a supporting, infrastructure activity.
- ✓ This organization may outsource its cybersecurity work to third parties to ensure proper safeguarding of data. It does not need to consider supply data sets that document highly specialized cybersecurity skills like network forensic analysis.
- ✓ Rather, this organization will track skills focused on cyber hygiene or information security, both skill sets that are easier to develop and for which to recruit.
- ✓ This organization does not have as great a need to grow cybersecurity professionals through experience and exposure to certain types of cybersecurity work.
- ✓ This organization will be less concerned with its cybersecurity professional pipeline because its supply requirements are minimal, and easily replaced through standard hiring or third party support.

Important supply data points for this quadrant could be:

- ✓ *Supply Characteristic:* Certification, specifically in Information Assurance and/or cyber hygiene.
- ✓ *Supply Characteristic:* Vacant positions, specifically current vacancies in IT positions.
- ✓ *Supply Characteristic:* Permanent and non-permanent employee types.
- ✓ *Supply Characteristic:* Grade, specifically supervisory status of cybersecurity workforce.
- ✓ *Supply Characteristic:* Specialized Skills represented by proficiency levels in the Oversight and Development category of Specialty Areas of the National Cybersecurity Workforce Framework.

Back to Supply Data

Supply Considerations - High Risk Exposure/Low Risk Tolerance

Leaders within the ***High Risk Exposure/Low Risk Tolerance*** organization can consider the following workforce implications:

- ✓ This organization has an imperative cyber mission and performs cybersecurity actions that take time for the workforce to acquire and perfect the necessary skills and abilities.
- ✓ Leaders should consider adverse impacts from cybersecurity breaches.
- ✓ Activities of cybersecurity professionals will require specialized cybersecurity data analysis. Also, the overall workforce requires varied mixes of skills in order to meet organizational mission requirements (e.g., digital forensics, all-source intelligence and data administration).
- ✓ As a result, types of supply data for this organization will include skills and experience mix, tenure, and succession pipeline.
- ✓ Leaders should also consider attrition, and retirement eligibility of its cybersecurity professionals.

Important supply data points for this quadrant could be:

- ✓ *Supply Characteristic:* Specialized Skills, specifically in Specialty Areas of the Investigate, Analyze, Operate and Maintain, and Securely Provision categories in the National Cybersecurity Workforce Framework.
- ✓ *Supply Characteristic:* Certifications, specifically in specialty areas like ethical hacking, reverse engineering, and penetration testing.
- ✓ *Supply Characteristic:* Vacant positions, specifically current and projected cybersecurity position
- ✓ *Supply Calculation:* Average retirement age of cybersecurity professionals.
- ✓ *Supply Calculation:* Time to hire, turnover rate, and recruitment pipeline.

Back to Supply Data

Contents

Evaluating Data Needs

Qualitative Management Tool

Risk Exposure

Risk Tolerance

Workforce Planning

Using The Diagnostic Tool

Step 1: Risk Exposure Ques.

Step 2: Risk Tolerance Ques.

Step 3: Diagnostic Matrix

STEP 4: Evaluating Supply and Demand Data

Conclusion

ITWAC Findings

Contact Us

Supply Considerations - High Risk Exposure/High Risk Tolerance

Leaders within the ***High Risk Exposure/High Risk Tolerance*** organization can consider the following workforce implications:

- ✓ This organization has an imperative cyber mission and performs cybersecurity actions that take time for the workforce to acquire and perfect the necessary skills and abilities.
- ✓ Leaders should consider adverse impacts from cybersecurity breaches.
- ✓ Activities of cybersecurity professionals will require specialized cybersecurity data analysis. Also, the overall workforce requires varied mixes of skills in order to meet organizational mission requirements (e.g., digital forensics, all-source intelligence and data administration).
- ✓ As a result, types of supply data for this organization will include skills and experience mix, tenure, and succession pipeline.
- ✓ Leaders should also consider attrition, and retirement eligibility of its cybersecurity professionals.

Important supply data points for this quadrant could be:

- ✓ *Supply Characteristic:* Specialized Skills, specifically in Specialty Areas of the Investigate, Analyze, Operate and Maintain, and Securely Provision categories in the National Cybersecurity Workforce Framework.
- ✓ *Supply Characteristic:* Vacant positions, specifically current and projected cybersecurity positions.
- ✓ *Supply Calculation:* Average retirement age of cybersecurity professionals.
- ✓ *Supply Calculation:* Time to hire and recruitment pipeline.

Back to Supply Data

Supply Considerations - Low Risk Exposure/High Risk Tolerance*

Leaders within the ***Low Risk Exposure/High Risk Tolerance*** organization can consider the following workforce implications:

- ✓ Cybersecurity activities are not central to the accomplishment of its mission, but rather a supporting, infrastructure activity (e.g., important in the conduct of transactional activity but not essential to the core function of the organization).
- ✓ This organization does not need a specialized cybersecurity workforce, and most likely would not identify a specific information security workforce either.
- ✓ Rather, this type of organization will minimally track skills focused on day to day operational ability of employing computer based technology (e.g., payroll, tracking inventory) and will therefore, not actively recruit individuals with cyber skills.
- ✓ Additionally, this type of organization does not grow cybersecurity professionals through experience and exposure to certain types of cybersecurity work (all of which takes time).
- ✓ Therefore, this organization is not concerned with nor does it track cybersecurity professional pipeline because in its view, it has no cybersecurity supply requirements.

Important supply data points for this quadrant could be:

- ✓ *Supply Characteristic:* peripheral cyber skills (e.g., ability to operate computer based technology).

* *There are very few organizations that fall within this quadrant. Many of these organizations include start-ups that are just beginning their business operations. As these organizations become more mature, they partner with other organizations more often, and will develop the need for more robust workforce planning.*

Back to Supply Data

Demand Considerations - Low Risk Exposure/Low Risk Tolerance

Leaders within the ***Low Risk Exposure/Low Risk Tolerance*** organization can consider the following workforce implications:

- ✓ Cybersecurity activities are a supporting, infrastructure activity but not central to mission.
- ✓ This organization may not need to prioritize potential demand by risk, but can determine tangible things in terms of work (i.e., drivers) that the cybersecurity workforce performs in its effort to accomplish its tasks (e.g., network faults that need correcting or patch installations that need to be performed).
- ✓ This organization may consider tangible data demand data drivers such as: number of networks to monitor, number of personal identity verification (PIV) or common access cards (CAC) to issue, user accounts to establish, etc.
- ✓ This organization will be able to determine the workforce level of effort (LOE) by calculating the amount of work it takes to complete one quantifiable driver (e.g., establish a user account) value.

Important supply data points for this quadrant could be:

- ✓ *Demand Driver Data:* Number of networks to monitor.
- ✓ *Demand Driver Data:* Number of hardware items to maintain.
- ✓ *Demand Driver Data:* Number of PIVs or CACs to issue.
- ✓ *Demand Driver Data:* Number of user accounts.
- ✓ *Demand Driver Data:* Historical number of cyber intrusions/attacks.

Back to Demand Data

Demand Considerations - High Risk Exposure/Low Risk Tolerance

Leaders within the ***High Risk Exposure/Low Risk Tolerance*** organization can consider the following workforce implications:

- ✓ Cybersecurity work is focal to the organization's business imperative, and it will always lack the resources needed to perform all work resulting from cybersecurity demand.
- ✓ As such, determining demand will require prioritizing potential cybersecurity threats.
- ✓ As a result, this organization will need to gather data that helps the organization determine a prioritization of the potential threats it faces.

Important demand data points for this quadrant could be:

- ✓ *Demand Prioritization Data:* Types of expected cyber attacks.
- ✓ *Demand Prioritization Data:* Characteristics of threat actors.
- ✓ *Demand Prioritization Data:* Average length of time attack lasts.
- ✓ *Demand Prioritization Data*: Threat conditions (i.e., historical number of potential cybersecurity threats and actual cyber intrusions/attacks.
- ✓ *Demand Prioritization Data*: Acceptable level of risk (i.e., level of impact [likelihood * probability] of cyber intrusion/attack).

Back to Demand Data

Demand Considerations - High Risk Exposure/High Risk Tolerance

Leaders within the ***High Risk Exposure/High Risk Tolerance*** organization can consider the following workforce implications:

- ✓ This organization has an imperative cyber mission and there will likely always be more work than the organization has resources.
- ✓ As such, determining demand requires not only determining tangible things in terms of work (i.e., drivers) that the cybersecurity workforce performs; but, more importantly, prioritizing potential cybersecurity threats.
- ✓ As a result, an organization with high risk will need to gather data that helps it prioritize of the potential threats it faces.

Important demand data points for this quadrant could be:

- ✓ *Demand Driver Data:* Number and type of regulations with which to comply.
- ✓ *Demand Driver Data:* Number of attack surfaces and number of external partners.
- ✓ *Demand Driver Data*: Number of likely cyber-attack actors.
- ✓ *Demand Prioritization Data*: Threat conditions (i.e., historical number of potential cybersecurity threats and actual cyber intrusions/attacks).
- ✓ *Demand Prioritization Data*: Acceptable level of risk (i.e., level of impact [likelihood x probability] of cyber intrusion/attack).

Back to Demand Data

Demand Considerations - Low Risk Exposure/High Risk Tolerance

Leaders within the ***Low Risk Exposure/High Risk Tolerance*** organization can consider the following workforce implications:

- ✓ Cybersecurity activities are not central to the mission, and are support infrastructure.
- ✓ This organization does prioritize its workforce demand by threats. Demand considerations include determining appropriate, quantifiable work that the cybersecurity workforce performs in its effort to accomplish its tasks (e.g., network faults that need correcting or patch installations needing performed).
- ✓ This organization may consider tangible data demand data drivers such as: number of help desk incidents to resolve and number of regulations to which to comply, etc.
- ✓ This organization may consider surge demand data as a result of absorbing cyber-attacks such as: work around, "fight through," and mission continuation activities.
- ✓ This organization will be able to determine the workforce level of effort (LOE) by calculating the amount of work it takes to complete one quantifiable driver (e.g., establish a user account) value and adding that to any defined surge demand.

Important demand data points for this quadrant could be:

- ✓ *Demand Driver Data:* Number of networks to monitor.
- ✓ *Demand Driver Data:* Number of help desk incidents to resolve.
- ✓ *Demand Driver Data:* Number of PIVs or CACs to issue.
- ✓ *Demand Driver Data:* Number of servers to disable due to absorbed cyber attack.
- ✓ *Demand Driver Data:* Number of trainings to attend for preparing individuals to "fight through".

Back to Demand Data

Contact Us

For additional information on the Cybersecurity Workforce Planning Diagnostic tool, please contact the Cybersecurity Education and Awareness Branch:

Homeland Security

Contact Information:
Kristina Dorville
Branch Chief, Cyber Education & Awareness
Department of Homeland Security (DHS)
Email: Kristina.Dorville@HQ.DHS.GOV
Phone:703-235-5761